Securing Service Provider Networks

IP Network Planes And Their Protection

Petr Pavlu (*ppavlu@cisco.com*)

This Session Scope/Purpose

- ## What it in

  - Set the context of the SP network security

  - Provide overview of the key concepts that need to be understood to set security policies and procedures

  - Set terminology and give starting point for further study and reading

- ## What it out

  - Exhaustive analysis of security risks, threats and attacks

  - Detailed explanation of techniques, tools, features used to secure networks

Agenda

- Internet Protocol Operation Fundamentals

- Types of Packets Handled by Routers

- Different IP Planes in Operation

- What Happens to IP Networks

- Securing IP Planes – Checklist of Key Concepts, Tools And Methods

- Summary And Further Reading

Agenda

- **Internet Protocol Operation Fundamentals**

- Types of Packets Handled by Routers

- Different IP Planes in Operation

- What Happens to IP Networks

- Securing IP Planes – Checklist of Key Concepts, Tools And Methods
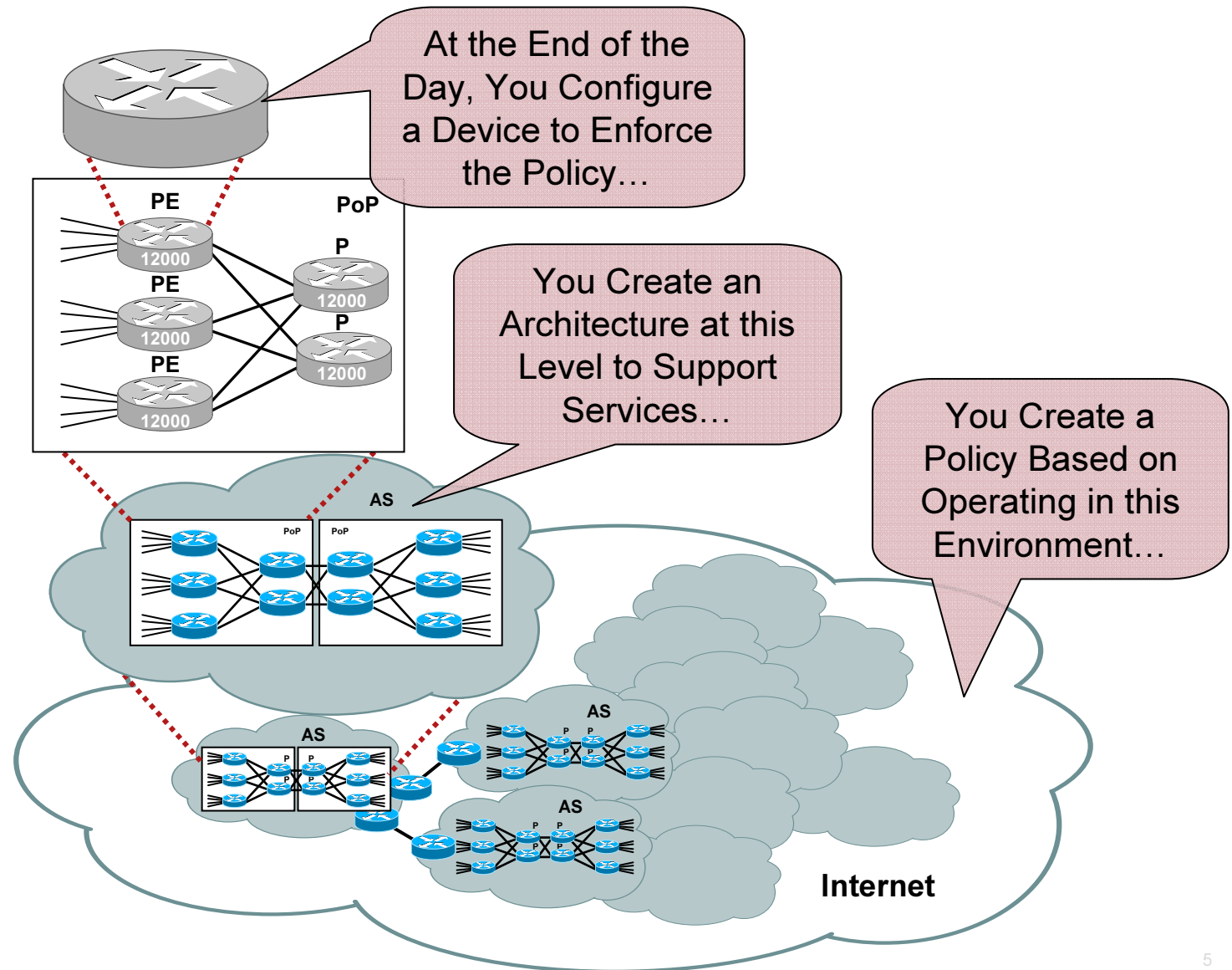
- Summary And Further Reading

Hierarchical Network Perspective…
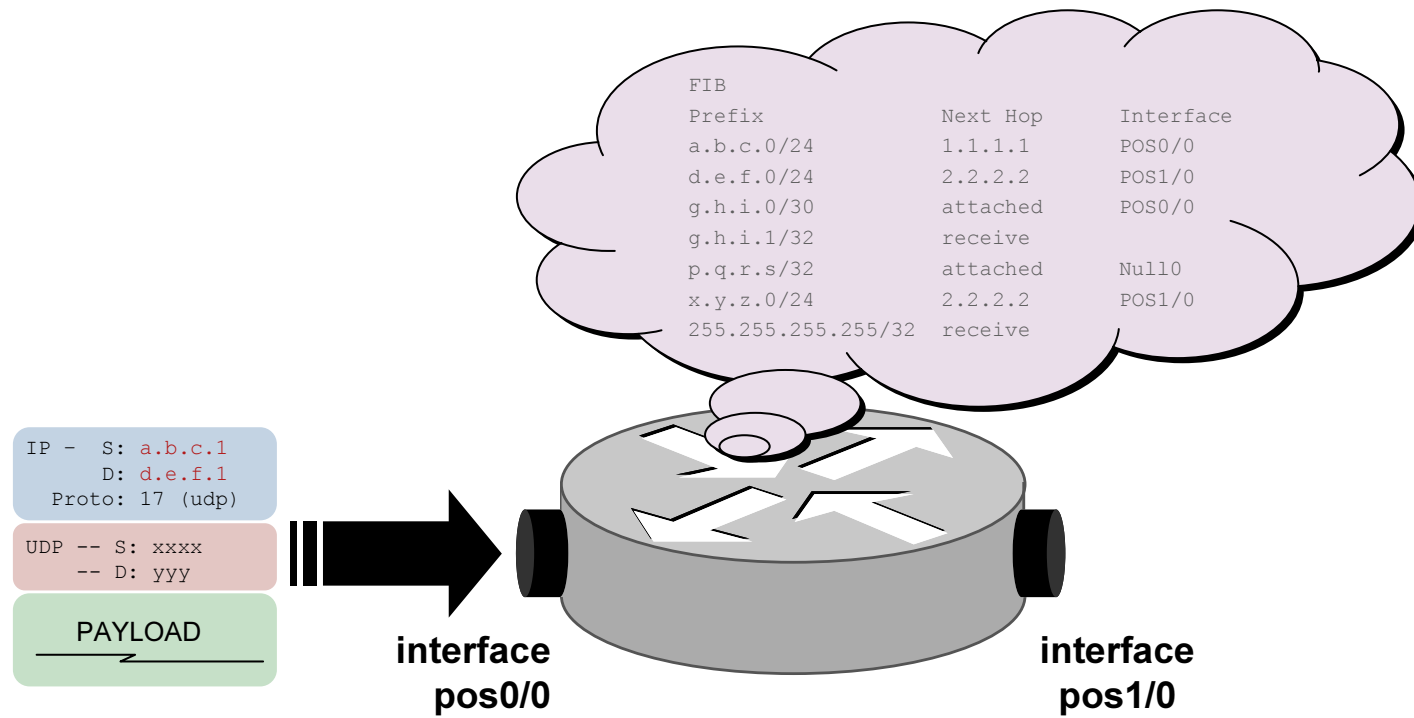

Router Perspective

PoP Perspective

AS Perspective

Internet Perspective

At the End of the Day, You Configure a Device to Enforce the Policy…

You Create an Architecture at this Level to Support Services…

You Create a Policy Based on Operating in this Environment…

It's All About the Packet

```
FIB
Prefix                Next Hop      Interface
a.b.c.0/24            1.1.1.1       POS0/0
d.e.f.0/24            2.2.2.2       POS1/0
g.h.i.0/30            attached      POS0/0
g.h.i.1/32            receive
p.q.r.s/32            attached      Null0
x.y.z.0/24            2.2.2.2       POS1/0
255.255.255.255/32    receive
```

```
IP -  S: a.b.c.1
      D: d.e.f.1
   Proto: 17 (udp)
```

```
UDP -- S: xxxx
    -- D: yyy
```

PAYLOAD

interface pos0/0

interface pos1/0

- Once a packet gets into the Internet, some device, somewhere has to do one of two things: [1] Forward the Packet* or [2] Drop the Packet

- In the context of security, the questions are more granular:

    –**Who** forwarded the packet, and **what** resources were required to do so…

    –**Who** dropped the packet, and **why** was it dropped…

* Forwarding Could Entail Adding a **Service** to the Packet as well…

Agenda

- Internet Protocol Operation Fundamentals

- **Types of Packets Handled by Routers**

- Different IP Planes in Operation

- What Happens to IP Networks

- Securing IP Planes – Checklist of Key Concepts, Tools And Methods

- Summary And Further Reading
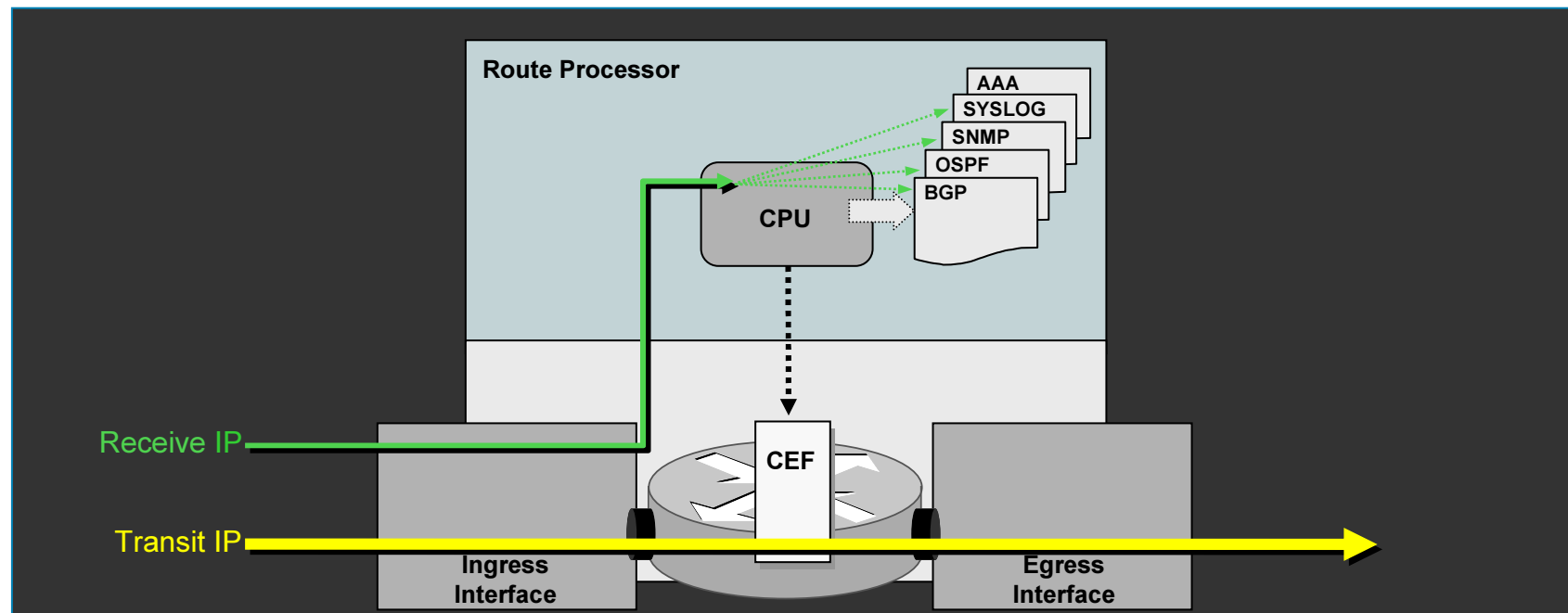
Transit Packets

Transit Packets

- Well-formed IP packets that follow standard, destination IP address-based forwarding processes. No extra processing is required to forward these packets.

- The destination IP address of these packets is located downstream from the network device and thus, the packet is forwarded out an egress interface

- Transit packets are handled by Cisco Express Forwarding (CEF), and (when available) by specialized forwarding hardware. The term "fast path" describes this type of forwarding.

Route Processor

AAA
SYSLOG
SNMP
OSPF
BGP

CPU

CEF

Transit IP

Ingress Interface

Egress Interface
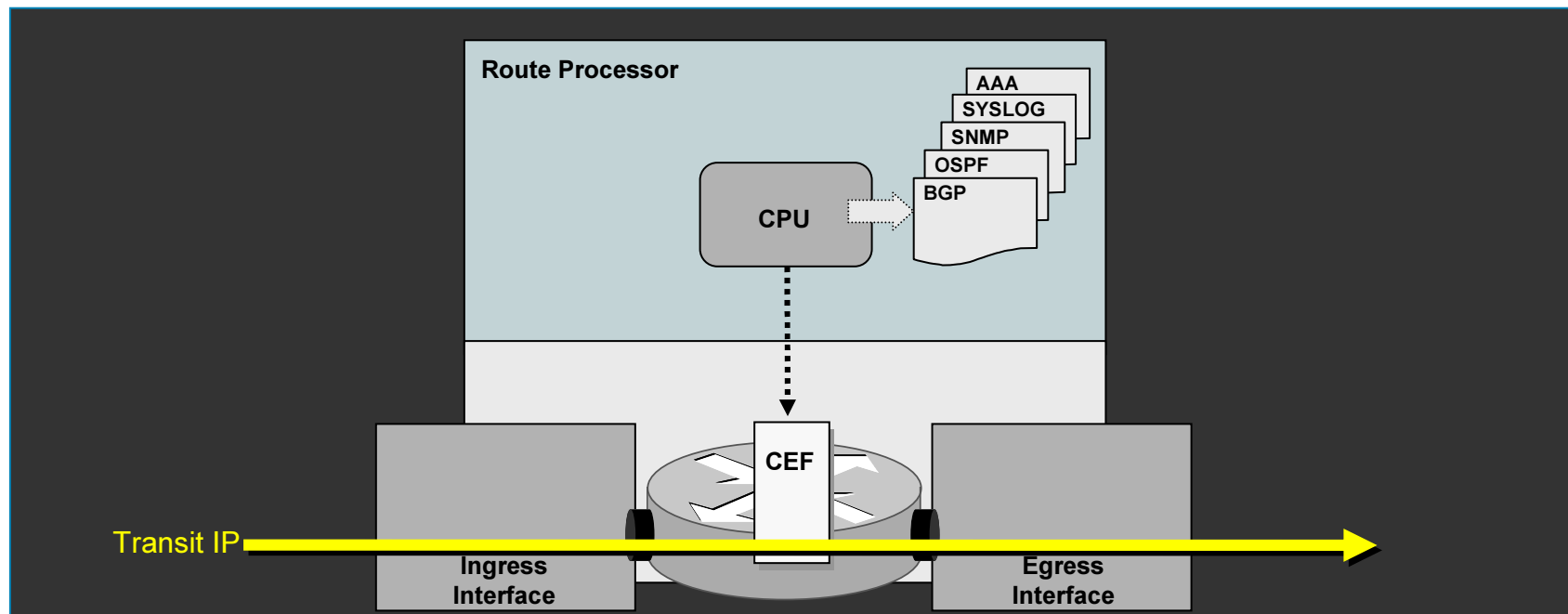
Receive Packets

Receive Packets

- Packets that are destined to the network device itself (e.g. control and management packets) must be handled by the route processor CPU since they ultimately are destined for and handled by applications running at the process level within Cisco IOS software

- The term "**receive**" is related to the way addresses belonging to the network device itself are marked in the CEF table, and the term "**punt**" is often used to describe the action of moving a packet from the fast path to the "punt path" in order to move the packet to the route processor for handling

Exceptions IP Packets

Exceptions IP Packets

- Exception IP packets include, for example, IPv4 packets containing IP header options, IP packets with expiring TTLs, and certain transit IP packets under specific conditions, such as the first packet of a multicast flow or a new NAT session

- All of the packets in this set must be handled by the route processor
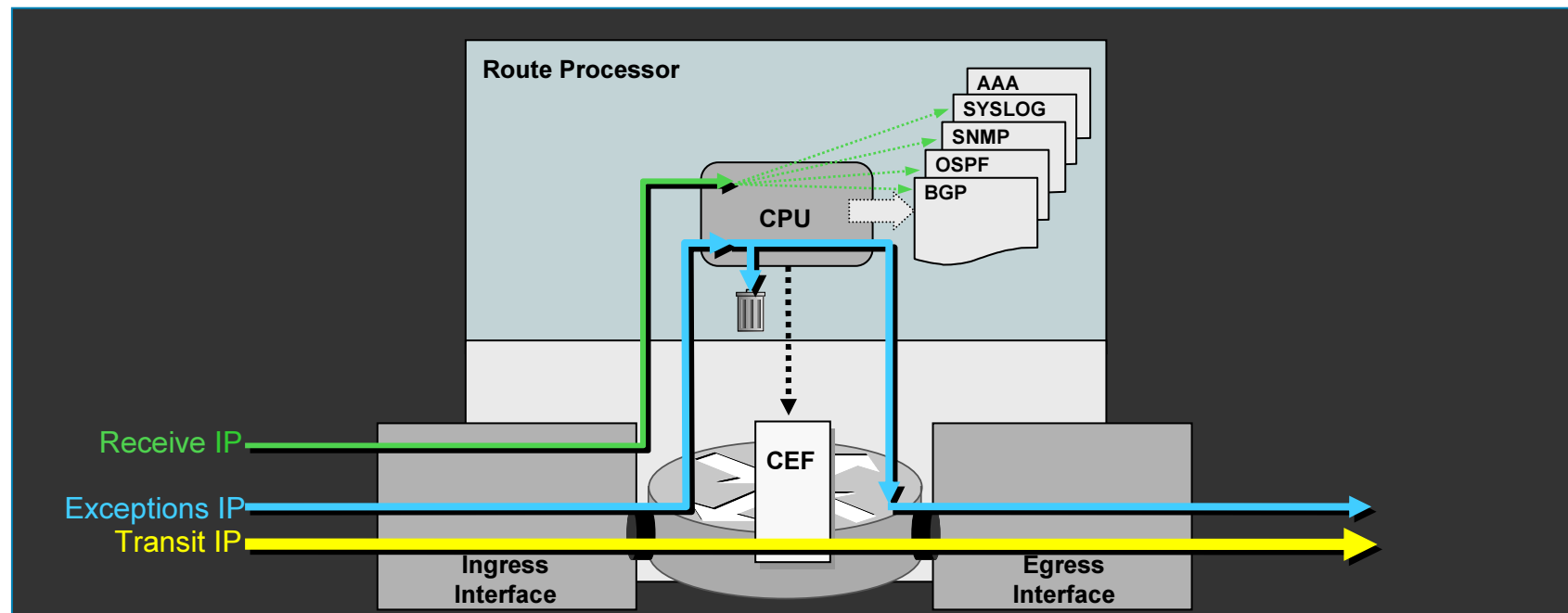
Non-IP Packets

Non-IP Packets

- Layer 2 keepalives, ISIS packets, Cisco Discovery Protocol (CDP) packets, and PPP Link Control Protocol (LCP) packets are examples of non-IP packets

- All of the packets in this set must be handled by the route processor
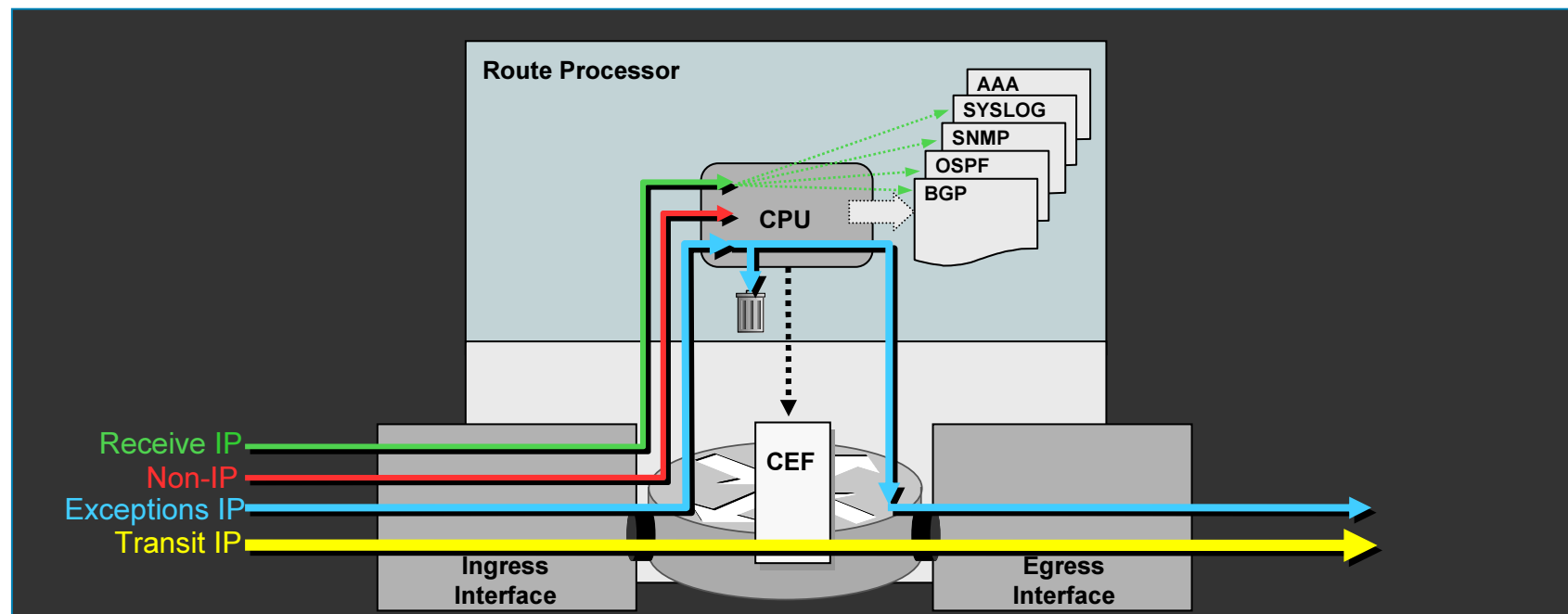
Agenda

- Internet Protocol Operation Fundamentals

- Types of Packets Handled by Routers

- **<u>Different IP Planes in Operation</u>**

- What Happens to IP Networks

- Securing IP Planes – Checklist of Key Concepts, Tools And Methods

- Summary And Further Reading

IP Data Plane

IP Data Plane

- The logical group containing all "**customer**" application traffic generated by hosts, clients, servers, and applications that are sourced from and destined to other devices, such as PCs and servers, that are supported by the network

- Data plane traffic is always be seen as **transit** packets by network elements. Most will be forwarded in the fast path; some may be "**exceptions IP**" packets.
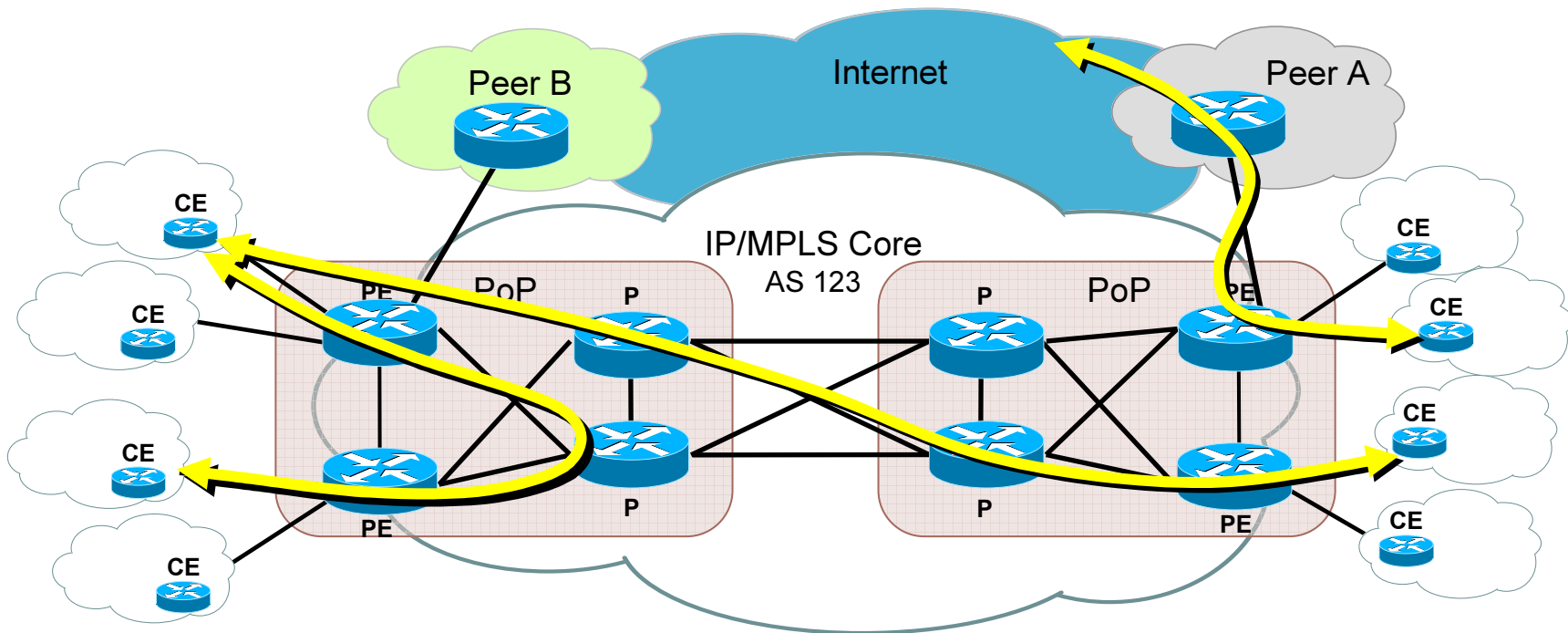
IP Control Plane

IP Control Plane

- The logical group containing all **routing**, **signaling**, **link-state**, and other control protocols used to create and maintain the state of the network and interfaces such as BGP, OSPF, LDP, IS-IS, and ARP, Layer 2 keepalives, ATM OAM, and PPP LCP frames, for example

- Control plane traffic always includes **receive** packets from the perspective of the src/dst network element, but logically includes certain transit packets (e.g., multihop eBGP) which are transit from the perspective of the intermediate routers along their path)
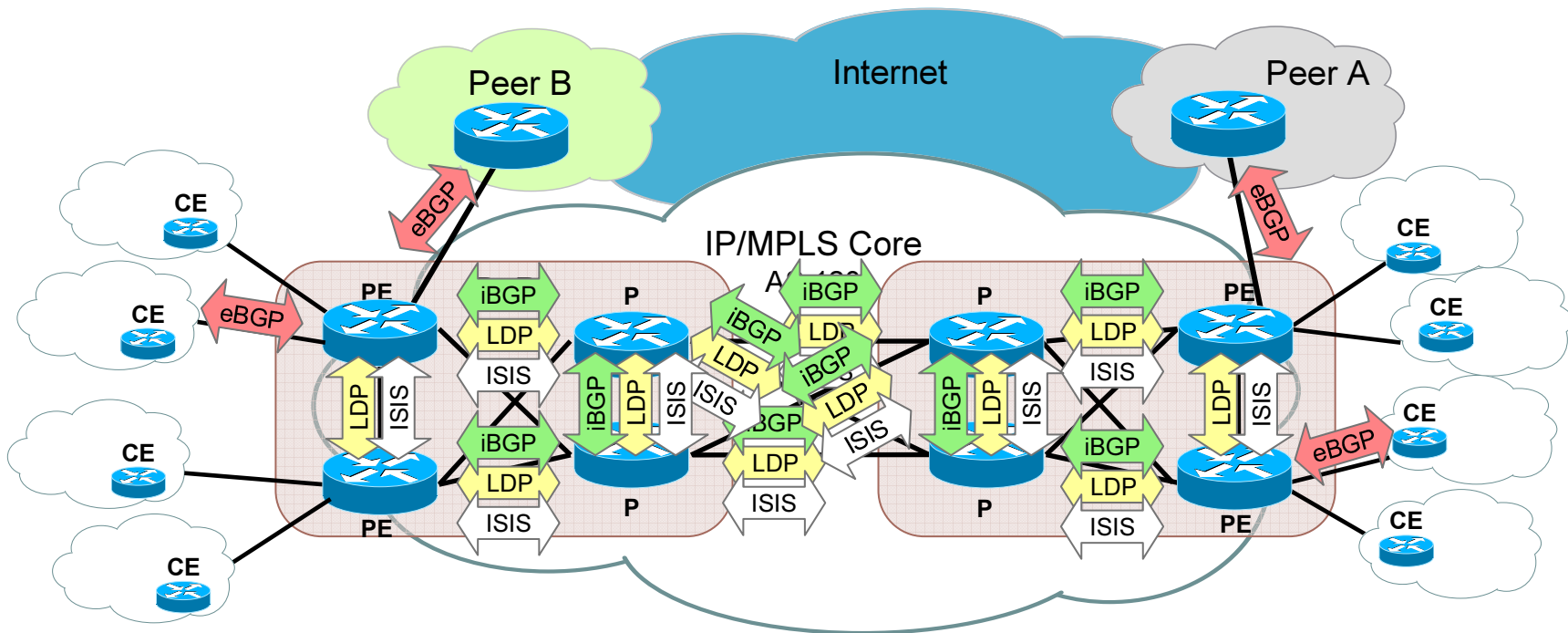
IP Management Plane

IP Management Plane

- The logical group containing all **management** traffic supporting provisioning, maintenance, and monitoring functions for the network. This includes traffic such as SSH, FTP, SNMP, Syslog, TACACS+ and RADIUS, DNS, NetFlow, ROMMON, CDP, etc.

- Management plane traffic always includes **receive** packets from the perspective of the src/dst network element, but logically includes certain transit packets (e.g. SSH packets which are transit from the perspective of the intermediate routers along their path)
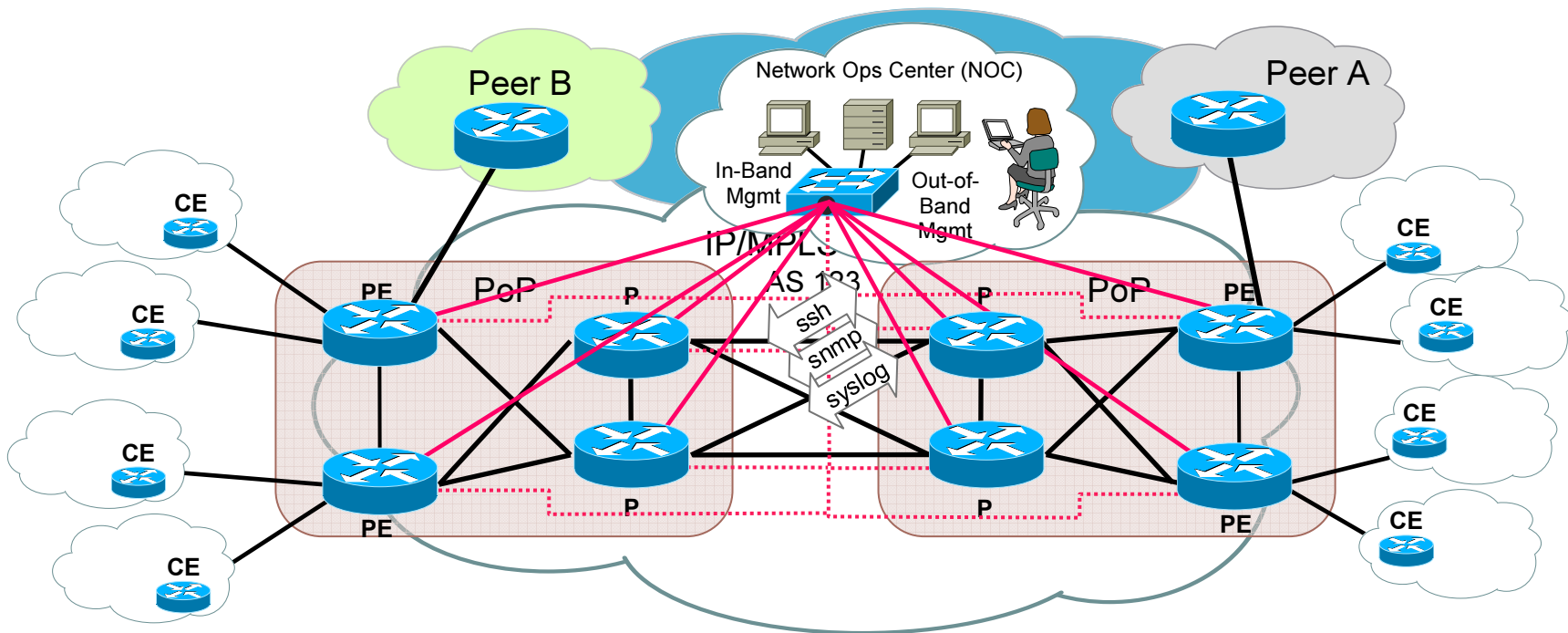
IP Services Plane

IP Services Plane

- The logical group containing "**customer**" traffic (like the data plane), but with the major difference that this traffic requires specialized forwarding functions applied it, and possibly consistent handling applied end to end. Examples include VPNs (MPLS, IPsec, and SSL), private-to-public interfacing (Network Address Translation [NAT], firewall, and intrusion prevention system [IPS]), QoS (voice and video), and many others.

- Services plane traffic is "**transit**" traffic, but network elements use special handling to apply or enforce the intended policies for various service types
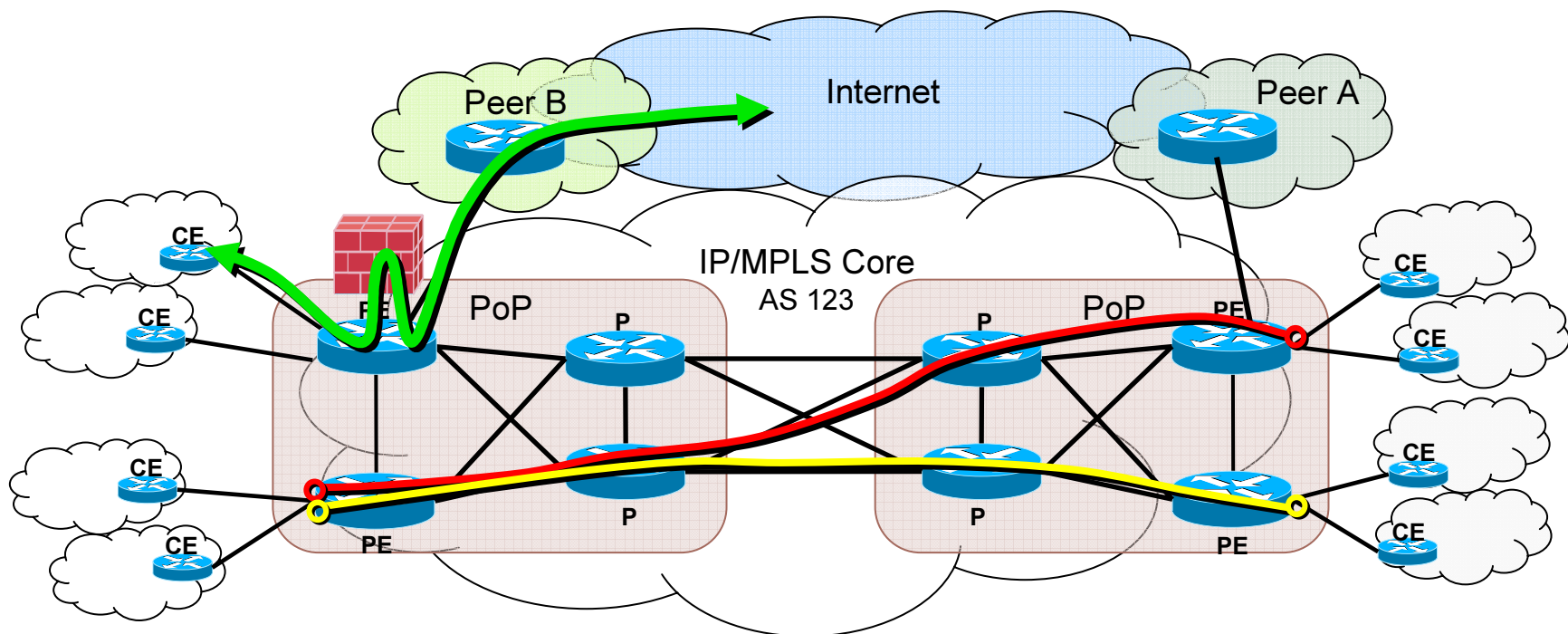
Agenda

- Internet Protocol Operation Fundamentals

- Types of Packets Handled by Routers

- Different IP Planes in Operation

- **<u>What Happens to IP Networks</u>**

- Securing IP Planes – Checklist of Key Concepts, Tools And Methods

- Summary And Further Reading

Threats Against IP Networks

- There are many factors that threaten network infrastructures…

  - Natural disasters

  - Unintentional, man-made attacks based on human error

  - Malicious attacks

- Clear distinction between human error and malicious attacks is intent

- Protection against malicious and unintentional attacks must both be considered

  - At the end of the day, an outage is an outage

Threat and Attack Models (1/2)

	Description
Resource Exhaustion Attacks	A Denial-of-Service (DoS) Attack that Aims to Make the Target Unavailable for Its Intended Service. May Be Attempted via a Direct, Transit or Reflection–Based Attack.
Spoofing Attacks	An Attack that Uses Packets that Masquerade Themselves with False Data, such as the Source IP Address, to Exploit a Trusted Relationship.
Transport Protocol Attacks	Attacks that Aim to Prevent Upper-Layer Communications Between Hosts, or to Hijack Established Sessions in Order to Capitalize on any Previous Authentication Measures, Enabling Eavesdropping and False Data Injection.
Routing Protocol Attacks	Attacks that Attempt to Destroy the Router's or Network's Ability to Perform Routing Tasks and, Thereby, Prevent New Routing Protocol Peering, Disrupt Current Peering, or Redirect Traffic Flows in an Attempt to Inject False Information, Alter Existing Information, or Remove Valid Information for the Purposes of Corrupting User Data.

Threat and Attack Models (2/2)

	Description
Attacks Against Other IP Control Plane Services	Attacks Against Important Control Plane Services such as DHCP, DNS, and NTP may Affect Network Availability and Operations.
Unauthorized Access Attacks	Attacks that Attempt to Gain Unauthorized Access to Restricted Systems and Networks.
Software Vulnerabilities	A Software Defect that, if Exploited, may Compromise the Confidentiality, Integrity and Availability of the Router and Associated Data Plane Traffic.
Malicious Network Reconnaissance	The Process of Gathering Information about a Target. Often Conducted in Preparation for an Attack; Enables the Attacker to Identify Specific Security Weaknesses that may Be Exploited as Part of a Future Attack.

Collateral Damage

- Attacks may have additional consequences beyond the intended target

- A denial-of-service (DoS) attack against one remote network may adversely affect other networks resulting in collateral damage and a wider impact

- Collateral damage must also be considered when evaluating risk

Bandwidth Concepts – PPS Engineering

- **What is the maximum frame rate for Gigabit Ethernet?**

  – The minimum frame payload is 46 Bytes (based on the slot time of Ethernet) and the maximum frame rate is achieved by a single transmitting node which does not suffer any collisions. This implies a frame consisting of 72 Bytes (see table below) with a 12 Byte inter-frame gap, for a total of 84 Bytes.

- **What is the maximum throughput for Gigabit Ethernet?**

  – The maximum frame payload is 1500 Bytes and the maximum throughput is achieved by a single transmitting node which does not suffer any collisions. Thus, a frame consisting of 1526 Bytes and a 12 Byte inter-frame gap, results in a total of 1538 Bytes.

```
      Frame Part                      Min Frame            Max Frame
   Inter Frame Gap (9.6ms)            12 Bytes             12 Bytes
   MAC Preamble (+ SFD)                8 Bytes              8 Bytes
   MAC Destination Address             6 Bytes              6 Bytes
   MAC Source Address                  6 Bytes              6 Bytes
   MAC Type (or Length)                2 Bytes              2 Bytes
   Payload (Network PDU)              46 Bytes           1500 Bytes
   Check Sequence (CRC)                4 Bytes              4 Bytes
                                   -----------           ----------
   Total Frame Physical Size          84 Bytes           1538 Bytes

   [1,000,000,000 bps/(  84 B * 8 b/B)] == 1,488,096 fps (max rate)
   [1,000,000,000 bps/(1538 B * 8 b/B)] ==    81,274 fps (min rate)
```

Bandwidth Concepts—PPS Engineering
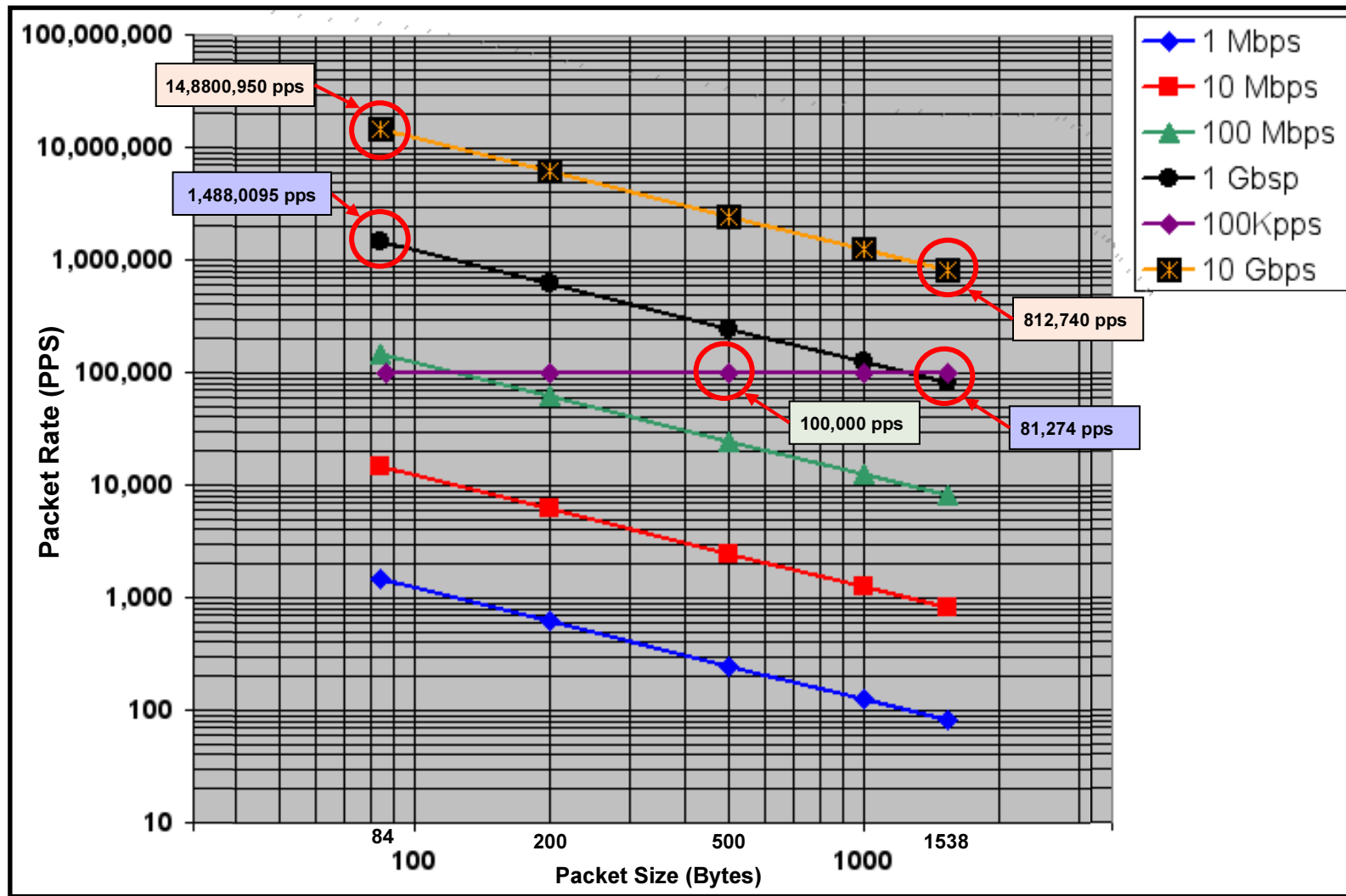
Bandwidth Concepts—PPS Engineering

- What are the relevant metrics for network engineering?

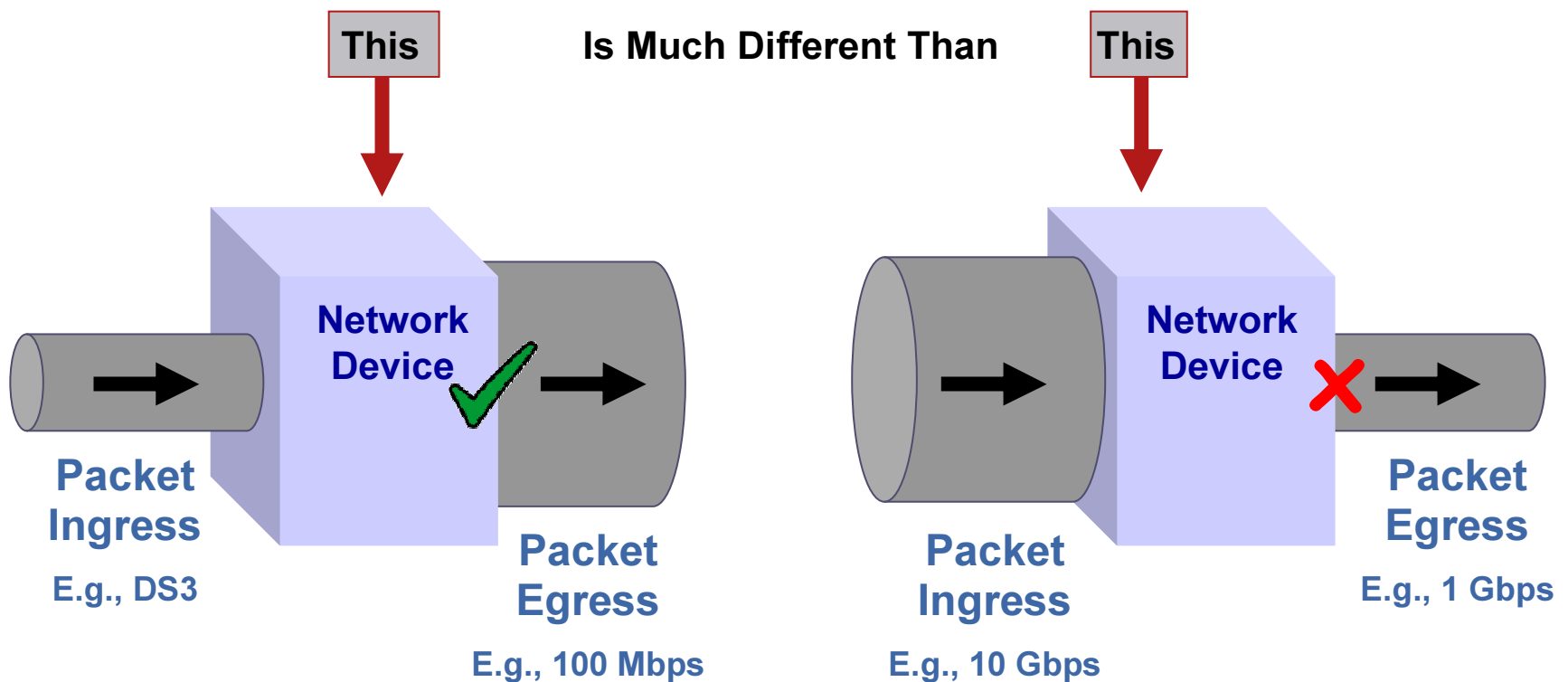|	
Bandwidth?...........................	Bits per Second… (bps).
Packet Rate?.......................	Packets per Second… (pps)
Connection Setup Rate?.......	Connections per second… (cps)
Transaction Rate?................	Transactions per second… (tps)
Total Number of Sessions?...	Concurrent connections… (cc)

- It depends…
  - What is the device type…
    - Stateless? Router, switch, etc.
    - Stateful? Firewall, IPS, load balancer, etc.
  - What environment is the device operating in…
    - Web Queries: short–lived, high connection rate, some state, PPS/CPS
    - Financials: short-lived, high transaction rate, high state, CPS/TPS
    - Video Streaming: long-lived, low connection rate, some state, PPS/concurrent conns
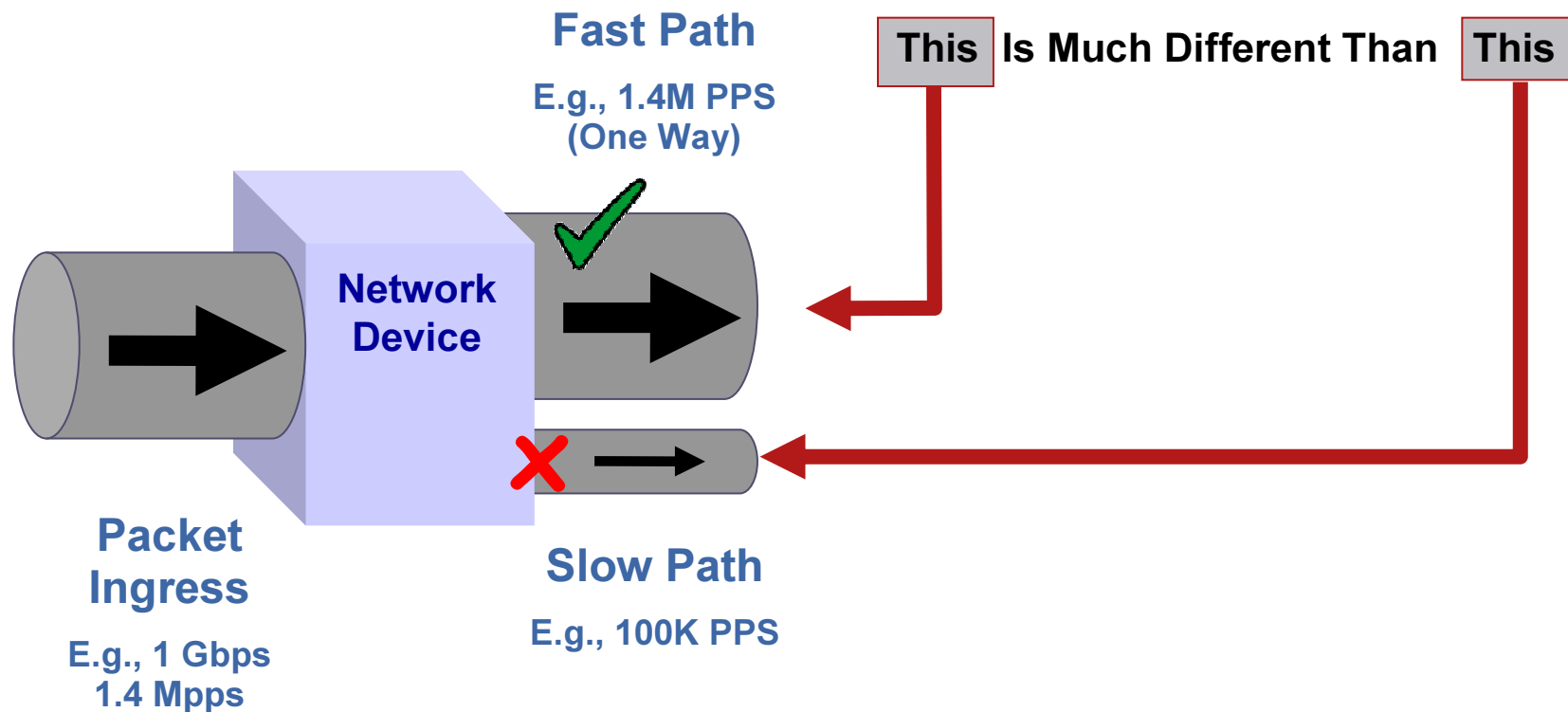   - VPN: long-lived, temporally high connection rate, high state, PPS/concurrent conns

Bandwidth Concepts—PPS Engineering

In **Network Design**, We Always Consider Bandwidth…

This	Is Much Different Than	This

Network Device ✔

Packet Ingress

E.g., DS3

Packet Egress

E.g., 100 Mbps

Network Device ✘

Packet Ingress

E.g., 10 Gbps

Packet Egress

E.g., 1 Gbps

Bandwidth Concepts—PPS Engineering

In Security Design, We Also Need to Consider PPS…

Fast Path

E.g., 1.4M PPS
(One Way)

This Is Much Different Than **This**

**Network
Device**

**Packet
Ingress**

E.g., 1 Gbps
1.4 Mpps

Slow Path

E.g., 100K PPS

Agenda

- Internet Protocol Operation Fundamentals

- Types of Packets Handled by Routers

- Different IP Planes in Operation

- What Happens to IP Networks

- **<u>Securing IP Planes – Checklist of Key Concepts, Tools And Methods</u>**

- Summary And Further Reading

IP Data Plane Security Techniques

- Interface ACLs

- Unicast RPF

- Flexible packet matching

- QoS techniques

- IP header option techniques

- IP routing techniques

IP Control Plane Security Techniques

- Disable unused control plane services

- ICMP techniques

- Selective packet discard

- IP receive ACL

- Control plane policing

- MD5 authentication

- BGP techniques

- Generalized TTL security mechanism

- Protocol specific filters

IP Management Plane Security

- Out-of-band management

- Password security

- SNMP security

- Remote terminal access security

- Disable unused management plane services

- Disable idle user sessions

- System banners

- Secure IOS file systems

- Role-based CLI access

- Management plane protection

- AAA

- AutoSecure

- Network telemetry

It is assumed that the network is physically secure.

Network-based security measures become ineffective if physical security has been breached.

IP Services Plane Security

- The IP services plane refers to user traffic that is treated by specialized handling beyond Best Effort Forwarding. This includes services such as:
  - QoS
  - VPNs (IPSec VPNs, MPLS VPNs, GRE, etc.)
  - Policy-based routing
  - SSL, firewall, IPS, NAT, etc.

- Services typically require the application of "premium" resources such as encryption/decryption, or extra CPU-processing
  - Premium services usually cost more to deploy and use finite-resources. Hence, premium services need to be 'protected' so that those who aren't paying don't get preferential treatment.

- Services must also be protected to prevent any one service from disrupting any other service, or best effort traffic form disrupting premium services

Agenda

- Internet Protocol Operation Fundamentals

- Types of Packets Handled by Routers

- Different IP Planes in Operation

- What Happens to IP Networks

- Securing IP Planes – Checklist of Key Concepts, Tools And Methods

- **Summary And Further Reading**

Key Takeaways

- IP network traffic can be segmented into four "traffic planes":
  - IP Data Plane
  - IP Control Plane
  - IP Management Plane
  - IP Services Plane

- Network elements have different handling processes, including a fast path and a slow path

- Design needs to anticipate the threats and attacks – in multiple different dimensions (bps, pps, sessions, transactions…)

- IP network traffic planes are protected by specific mechanisms, and when combined, provide a defense in depth and breadth approach to securing IP networks

Recommended Reading

http://www.ciscopress.com/bookstore/product.asp?isbn=1587053365
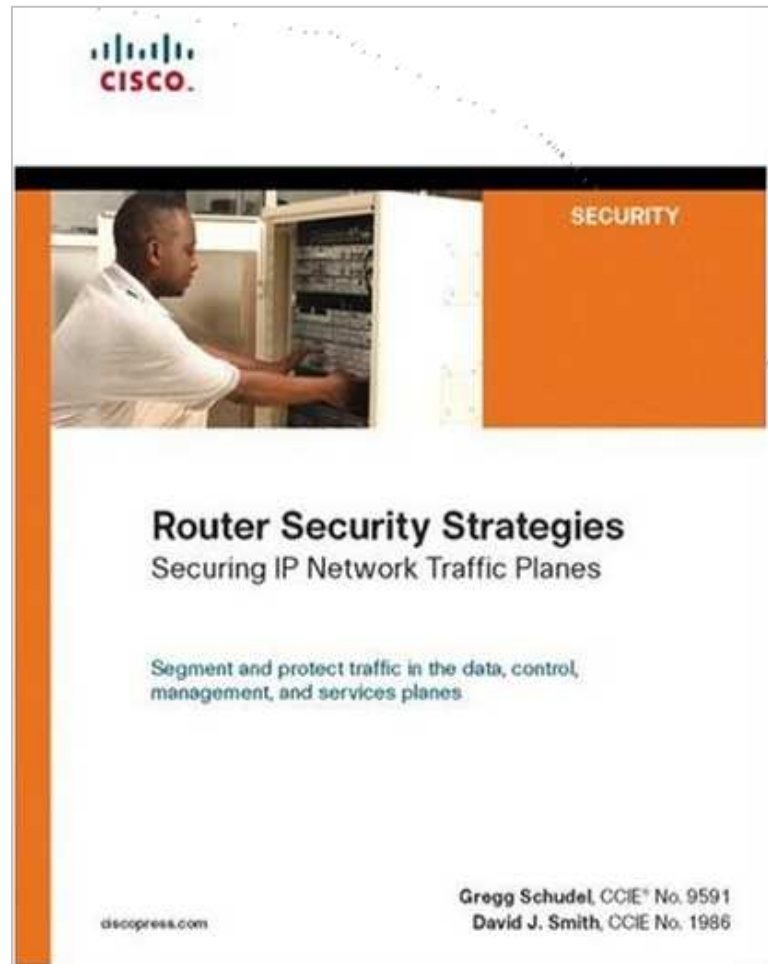
Cisco Networkers Barcelona
26 – 29. January 2009.
Register now!

http://www.cisco.com/web/europe/cisco-networkers/2009/index.html